DEPARTMENT OF THE ARMY
HEADQUARTERS, UNITED STATES ARMY MATERIEL COMMAND
5001 EISENHOWER AVENUE, ALEXANDRIA, VA 22333-0001

AMC Supplement 1 1 December 2000
to AR 380-19

Security

INFORMATION ASSURANCE

This supplement prescribes policy, assigns responsibility, and establishes procedures for implementing supplemental security requirements for automated information systems, Army Materiel Command (AMC) wide. This supplement further delineates responsibilities and defines procedures for Headquarters (HQ), AMC; AMC major subordinate commands (MSCs), and separate reporting activities (SRAs); AMC project/product managers; separate installations and activities reporting directly to HQ AMC; and Government owned, contractor-operated (GOCO) activities under AMC jurisdiction that process sensitive-but-unclassified (SBU) information. This supplement provides for the implementation of security measures for all AMC-operated automated information systems (AISs). Commanders, managers, Chief Information Officers (CIOs), and Information Assurance Managers (IAMs) will ensure that security measures are implemented to provide optimum security for all automated systems within their areas of responsibility. This supplement may be further supplemented by AMC MSCs, SRAs, installations, and activities reporting directly to Headquarters, AMC, as required, subject to HQ AMC approval (AMCIO-F), prior to implementation. One copy of each supplement will be furnished to the Commander, USAMC, ATTN: AMCIO-F, 5001 Eisenhower Avenue, Alexandria, VA 22333-0001, and the AMC Intelligence and Technology Support Activity, ATTN: AMXMI-SD, 1323 Cobb St. SW, Fort McPherson, GA 30330-5000.

AR 380-19, 27 February 1998, is supplemented as follows:

Page ii, Appendixes. Add the following:

H. Memorandum of Agreement
I. Certification, Accreditation and Reaccreditation
J. Minimum Accreditation Documentation Required
K. Minimum Criteria for Connection to AMC Network Infrastructure

Page 1, paragraph 1-1c, Purpose. Add subparagraph (6) after subparagraph (5).

(6) Contracts for facilities processing sensitive-but-unclassified (SBU) defense information will specify requirements of the basic regulation, AR 380-67, and this supplement. Operation and accreditation authority will remain within the AMC chain of command for AMC-owned systems.

Page 3, paragraph 1-4f(2). Add the following at the end:

The Commander, AMC will appoint the Information Assurance Program Manager (IAPM) (formerly called the Information Systems Security Program Manager). MSCs are authorized to appoint MSC IAPMs based upon

*This supplement supersedes AMC Supplement 1 to AR 380-19, 28 September 1993 the size of the command. An MSC may appoint an IAPM if the MSC contains five (05) or more subordinate activities.

Page 4, paragraph 1-4. Add subparagraph k after subparagraph j.

k. The AMC IAPM is responsible for functioning as the central point of contact (POC) for information from and to the Information Assurance Manager (IAM), (formerly known as the Information Systems Security Manager (ISSM)); the Information Assurance Network Officer (IANO), (formerly known as the Network Security Officer (NSO)); and all authorized users. The chain of command for reporting any IA problem will be from the bottom up. The IAM is responsible for maintaining control of all AMC assets within the area of the installation’s local area network (LAN)/wide area network (WAN) configuration. The IAM can require tenants to provide any special equipment necessary to support the tenant requirements for network connection.

Page 4, paragraph 1-4. Add the following subparagraphs (1) and (2) after subparagraph 1-4k.

(1) The IANO is responsible for coordinating security activities for the IAPM, ensuring command-wide security of the network infrastructure, identifying all interfaces to the network infrastructure, coordinating with IAMs in developing appropriate security policies, and implementing the infrastructure security policies.

(2) The IANO is responsible for enforcing the AMC network infrastructure connectivity policy, and generating and implementing procedures at the network level for System Administrators (SAs). The IANO ensures the network and underlying hosts are operating securely; notifies the Information Assurance Security Officer (IASO), (formerly known as the Information Systems Security Officer (ISSO)) of any modification to the security status prior to implementing the modification; and ensures each host has implemented basic security mechanisms prior to connectivity to the installation network. Each IANO coordinates with the IASO on security related issues. The IANO identifies all communication interfaces to the installation infrastructure; implements security features built into the component hardware; maintains the configuration of AMC networks; maintains the network mapping; maintains the current SA POC list; verifies SA compliance; and audits network devices.

Page 4, paragraph 1-4. Add subparagraph l after subparagraph k.

l. All authorized user responsibilities. All authorized users of the network must notify the designated IASO upon observation of actions that conflict with the AMC network infrastructure connectivity. Users are responsible for protecting AMC assets, including information systems equipment, data, and information regardless of the security mechanisms that are in place.

Page 4, paragraph 1-5b(1)(f). Add the following sentence:

Information related to equipment and materiel undergoing research, development, test, and evaluation (RDT&E); certain related information concerning defense efforts on special projects (i.e., weapons systems, etc.); and the devices needed to provide protection for data contained in the computer system as determined by the proponent of the information and appropriate security manager, will refer to chapter 4 for specific guidance concerning types of information to be protected and restraints imposed on protection measures.

Page 4, paragraph 1-5g. Add subparagraph h. after subparagraph g.

h. The following are AMC management, function, and security goals:

(1) Maintain a network that connects the entire installation’s AMC resources and tenant units on a single installation-wide backbone.

(2) Provide an installation-level primary point of access to the Unclassified but Sensitive Internet Protocol Routing Network (NIPRNET) and centralized network management for the AMC installation infrastructure. In some cases provide a single, centralized, electronic mail (Email) system to AMC installations and tenant units; a single, centralized World Wide Web (WWW) server; some centralized data storage capability; a network for AMC operational use; and a mobile user support in accordance with current DA regulations, memorandums, and policies.

(3) Ensure the AMC elements and other tenant networks attached to the AMC backbone present no significant risk to the backbone and each other.

Page 5, paragraph 1-6d(2). Add the following after the first sentence:

At the MSC/SRA level, commanders/directors will appoint an IAM. At the installation level, an IASO need only be appointed. Where the MSC is also the host activity on an installation, the IAM assigned at the MSC level may also be the IAM for the installation. Commanders of AMC tenant activities on AMC installations may appoint an activity IAM to oversee the activity IA program and to support the installation IAM on conduct of his/her responsibilities under provisions of paragraph 1-6d(2). AMC tenant activities on a non-AMC installation will appoint an activity IAM unless prohibited by host installation command regulation. The MSC IAM must keep records on Management Decision Packages (MDEP) for MS4X (IA funds) expenditures and provide the AMC IAPM with an annual accountability report during the last quarter of the fiscal year. IAMs are required to keep record of all those system administrators who have been certified. The IAM is responsible for defining and enforcing the AMC installation security policy for the DAA.

Page 5, paragraph 1-6d(3)(a). Add the following at the end of the sentence:

The IASO will enforce the AMC network infrastructure connectivity policy.

Page 5, paragraph 1-6d(3)(e). Add the following after the last sentence:

Post all security officer appointments in an area with visibility.

Page 5, paragraph 1-6d(3)(k). Add the following at the end:

This function may be delegated, provided the individual performing this function has been delegated password management in writing.

Page 5, paragraph 1-6d(3)(m). Add the following at the end of the last sentence.

Grant access to the AMC installation network.

Page 5, paragraph 1-6d(3). Add subparagraphs (p) through (r) after subparagraph (o).

(p) The IASO will designate a specific number of days before disabling inactive accounts and ensure retirement of the affected user id’s and passwords (coordination with SA required).

(q) Maintain the configuration management of network assets within their designated area of control.

(r) Posting all security officer appointments in an area with noticeable visibility.

Page 5, paragraph 1-6d(4). Add subparagraphs (a) through (i).

(a) Identify all communications interfaces and connection requirements to include all modems/modem owners.

(b) Install and maintain command and control (C2) protect tools, account management, and auditing in accordance with current regulations or directives as required.

(c) Install and maintain all security patches and service packs that are provided by the software vendor or any authorized DoD source, as directed.

(d) Establish and maintain a strong password policy that requires passwords to be changed every 6 months or less.

(e) Ensure that auditing tools are in place, configured properly, and results reviewed weekly.

(f) If possible, run software tools like "CRACK" monthly to check for password quality. If necessary, lock out those users with non-compliant passwords.

(g) Ensure secure system setup and operation.

(h) Notify the IASO and obtain approval prior to making significant or security-related system configuration changes.

(i) Notify the local IANO and IASO of any compromises in accordance with requirements set in AR 380-19.

Page 7, paragraph 2-3a(1). Add the following at the end of the next to the last sentence:

Within AMC, audit information will be retained for at least 90 days.

Page 7, paragraph 2-3a(12). Add subparagraph (13).

(13) Continuity of Operations Plan. All AISs are required to develop, test, and maintain a Continuity of Operations Plan (COOP) in accordance with DA PAM 25-1-1. The COOP will be designated and tailored to be proportionate to the complexity and criticality of the systems supporting the specific concept of operations.

Page 8, paragraph 2-4b. Add subparagraphs (1) through (9):

(1) For auditing purposes, government or contractor personnel authorized to use commercially licensed software must be able to produce the original diskettes/compact discs (media) and documentation or, in the case where a multi-user or site license applies, a copy of the applicable license. Once the software has been installed, the original software will be protected from damage and theft by storing in an approved manner/area. The documentation should be afforded reasonable protection, but not necessarily to the same degree as the software.

(2) No government-procured or leased software shall be removed from the organization without the written approval of the IASO. Software shall not be removed from the installation without the regulatory completion of OF Form 7 (Property Pass) (see AR 1-39, Defense Supply Service-Washington). All users will comply with copyright laws/licensing agreements.

(3) Government-procured or leased software will not be used for personal profit or gain.

(4) Use of privately owned commercial, public domain, freeware, or shareware software on Government owned equipment is discouraged, but may be permitted if the government cannot provide the appropriate software to the user. An authorization request will be forwarded through the immediate supervisor to the IASO. The IASO will approve the request if it is for use of software that will not conflict with or corrupt Government owned resources. The installation DOIM/CIO and the IAM may be requested to assist the IASO in determining the acceptability of the software package. If the approval is granted, the IASO must provide the user with written authorization for use of the software package to satisfy audit requirements. Prior to its use, the software will be verified to be free of any bugs or viruses. The authorization will be written and signed by the IASO and included in the hardware/software inventory list. Additionally, the following conditions will be met:

(a) Does not violate license/copyright constraints.

(b) Is used only for government work.

(5) Government-procured or leased copyrighted software will not be loaned or borrowed. Software may be tested by others to determine future use, possible purchase, etc., only if expressly permitted in vendor license agreements.

(6) Government-procured or leased software will be accounted for and a central point of contact will be established to reduce duplication.

(7) Licensed software will be properly registered with the supplier (e.g., by the person to whom the software is initially issued or by the IASO). The IASO will ensure this function is accomplished. For network operations, a single point of contact for each network will be established to distribute software updates to applicable network sites/workstations.

(8) When older versions of commercial software packages are upgraded, the superseded software media must be disposed of properly. Unless vendor license agreements specify disposal procedures for obsolete software, the obsolete diskettes will either be cut in half or burned, or purged and reformatted. Compact discs (CDs) will be disposed of by breaking CDs in half or thoroughly scratching surface containing software data.

(9) Software declared as excess will be turned in to the supporting installation DOIM/CIO for reissue or disposition.

Page 8, paragraph 2-4f. Add subparagraphs (1) through (3).

(1) Copyrighted software may only be copied as explicitly set forth in the contract under which acquired (see DoD Federal Acquisition Regulation Supplement (DFARS) at 227.71 and 227.72 and under the following conditions:

(a) Preparing backup copies for operational and archival purposes per Title 17, U.S. Code (USC), Section 117, "Limitations on Exclusive Rights: Computer Programs." Prepared copies should be tested to ensure that true duplicates of the original have been made. A backup copy should then be maintained in a separate, secure place at the user installation.

(b) Duplicate copies that are kept at COOP sites must be maintained in a manner equal to the original data medium.

(2) Control of government-licensed commercial software will be maintained in accordance with AR 25-1, paragraph 5-3.c.

(3) Government-developed software: Software developed by a government employee as a part of his/her duties is owned by the government and no copyright may be obtained. For more information, see AR 27-60 (Patents, Inventions, and Copyrights).

Page 8, paragraph 2-4. Add subparagraphs h. and i. after paragraph g.

h. Unauthorized software.

(1) All unauthorized or undocumented software found during inspections will be removed from the equipment (the first-line supervisor with IASO assistance, if necessary, will ensure that the software is erased from the hard disk).

(2) Repeated occurrences of unauthorized software being found will be reported to the IAM and appropriate management for consideration of disciplinary action against the offending user.

i. In those instances where precluding operator access to application programs and system functions is not practical, audit trails will be provided for all access and attempted access.

Page 8, paragraph 2-6a. Add the following at the end of the paragraph.

The Army Computer Emergency Response Team (ACERT) at the Land Information Warfare Activity (LIWA) is the tool distribution point for the Army. C2 protect tools as well as McAfee and Symantec's Norton Anti-Virus tool suites are available to the Army through the ACERT web site at http://www.acert.belvoir.army.mil or ftp://ftp.acert.belvoir.army.mil. System administrators are encouraged to download the mandated C2 protect tools, as well as review and install other security related tools available at this site for the security of their information systems. All systems within the scope of this policy will utilize the C2P tools that apply to their environment.

(1) Exception to Approved C2P Tool List. If, after careful consideration, an SA recommends that one or more of the tools not be utilized on a system, the SA must present documentation which:

(a) Describes the system to be exempted to include its users and connectivity,

(b) Identifies which applicable tool(s) should not be used, and

(c) Provide justification for the recommendation.

(1) Waiver justifications may be based upon a risk assessment (confirmed by DAA) or redundancy of C2P tools with installed protections.

(2) Externally controlled systems that operate at AMC installations should reflect that the system proponent was notified of the AMC policy. A copy of the notice should be included.

(2) Accreditation. These tools are required for accreditation purposes. The operational use or non-use will be addressed in each system security plan/documentation submitted to a DAA for approval. If a system security plan identified the need for the operational use of any C2P tools in support of the system implementation, the tools will then also be used in the security and evaluation/security certification phase of the accreditation process. Results from running the tools as part of the security test and evaluation (STE) will be included in a STE report which is to be enclosed as an annex to the final system security plan/documentation and request forwarded to a DAA for review and approval. C2P tools implementation and changes must be reported within 90 days of their implementation.

(3) Accountability. The organization IAM must maintain a list of all systems and their status regarding tool implementation. This information must be forwarded annually to the AMC IAPM. Documentation regarding exceptions should be forwarded to the AMC IAPM.

Page 8, paragraph 2-7. Add subparagraph e after subparagraph d.

e. The above operational procedures will be implemented as appropriate by the accreditation authority based upon mission essentiality/vulnerability of the individual AIS. Where necessary, a classified program audit officer (CPAO) will be appointed by the IAM to accomplish the procedures prescribed in application software processing classified data. For scientific and engineering applications, this responsibility may be assigned to the appropriate level of project leadership to act as the CPAO. The CPAO is responsible for reporting discrepancies of the AIS to the IAM.

Page 9, paragraph 2-10. Add subparagraphs j and k after i.

j. Physical security measures for protection of support facilities will be as determined by the local commander.

k. The accreditation authority will approve all physical security waivers applicable to this supplement and the basic regulation. All physical security requirements requiring waivers will be coordinated with the installation physical security officer prior to submission to the accreditation authority for approval. These waivers will be included in the appropriate accreditation document. Physical security waivers that require HQ AMC approval will be forwarded to HQ AMC, ATTN: AMCPE-S. Information security storage waivers that require HQ AMC approval will be forwarded to HQ AMC, ATTN: AMCMI.

Page 9, paragraph 2-11. Add subparagraphs d through m after subparagraph c.

d. Some operating environments may require the use of locking devices to prevent unauthorized use of small computers. For AISs to which this applies, procedures will be established per AR 190-51.

e. Implementation of key access control procedures will be documented in the AIS SOP.

f. Basic responsibility will be placed with the user who has control of the information, has the need to protect it, and has the necessary authority and resources (i.e., the primary user of the small computer). Commanders and supervisors, with advice from the IASO, must ensure that these responsibilities are met.

g. The users of small computers are responsible for the equipment, media, and data processed on their small computer, to include

(1) Properly securing all information and media to protect against unauthorized access, destruction, or damage.

(2) Labeling reports generated to identify and differentiate the sensitivity of information as well as the creator's name and date of processing.

(3) Properly documenting programs to facilitate their turnover to new users.

(4) Reviewing and complying with software licensing agreements.

(5) Making backup copies of files and programs.

h. Access Controls: Most small computers are intended for a single user, which results in minimal built-in security features. Where a single person is using a small computer, adequate physical controls can be used to control access. Problems arise, however, when a single small computer is shared by several users, all of whom may not have the same need-to-know for the information stored in permanent storage. If access control programs are not, or cannot be, used, storage media will be removed and memory cleared when the system user changes.

i. Physical and administrative controls provide a cost-effective means of controlling access to the small computer and its information. An unauthorized user could unintentionally destroy or compromise valuable information by "playing" with an unattended machine. Although these controls tend to be less consistent (because they depend upon people for their execution), they are usually relatively easy and inexpensive to implement. Several types of access control mechanisms used to control the use of small computers include the following:

(1) Magnetically encoded "key cards" that perform a function similar to physical key-locks and that can provide additional coded information.

(2) Logging off when not in use or when unattended.

(3) Use of start-up programs that take control of the computer automatically (when the small computer is turned on or a new user logs on) until the user can be verified.

(4) Programs that maintain control at all times by limiting users to predefined functions.

(5) Password protection for programs and files.

(6) Read-only file protection.

(7) Use of existing software-provided passwords or keys.

(8) Use of screen saver password.

j. Small computers do not normally provide a mechanism to determine user identification. Consequently, programs must be purchased separately to provide this level of security. For situations in which several users share a single small computer, user authorization and identification should be authenticated in some manner.

k. Examination, monitoring, and supervision of usage are desirable security features which may be acquired through automated or manual means. Programs can be developed or purchased that will record usage information. A reliable source of date and time information (e.g., an internal clock calendar) and protection of this audit information from modification or destruction would also be needed. The types of events that may be of interest include:

(1) System start-up.

(2) User log on and log off.

(3) Job start and finish.

(4) User file access.

l. A current inventory of small computer equipment should be maintained and annually validated with the appropriate property custodian, as applicable, per AR 710-2 (Supply Policy Below the Wholesale Level).

m. Environment. Smoke, dust, and other contaminants can easily damage many components of a typical small computer. Measures to reduce environmental hazards include the following:

(1) Keep areas clean where small computers are located.

(2) Do not permit eating, drinking, or smoking in the immediate area of the AIS.

(3) Keep the small computer away from open windows, direct sunlight, radiators, and heating vents.

(4) Provide a permanent location for the small computer on a solid, stable desk or table.

<u>Page 10, paragraph 2-14e</u>. Add subparagraph (5).

(5) Automatic account/password expiration due to inactivity.

<u>Page 10, paragraph 2-15</u>. Add the following to the end of subparagraph b.

Security training will be accomplished in accordance with the AMC-issued Information Assurance Training Policy Memorandum #98-01, dated 16 Jul 98.

<u>Page 11, paragraph 2-16b</u>. Add the following at the end.

All contracts will reflect security investigation (access) requirements per AR 380-67, paragraph 3-401, and identification of position sensitivity designations as determined per AR 380-67, paragraph 3-101.

<u>Page 11, paragraph 2-16b(1)</u>. Add the following at the end.

For positions designated as critical-sensitive because of Category I ADP responsibilities, DD Form 1879 (DOD Request for Personnel Security Investigation) will be used. The Defense Security Service (DSS) will then perform a Single Scope Background Investigation and issue a TOP SECRET clearance. This investigative requirement is valid even when individuals appointed to such positions do not require access to TOP SECRET information. Similarly, for positions designated as non-critical sensitive because of Category II ADP responsibilities, DSS will perform the appropriate investigation as the basis for issuing a SECRET clearance. DSS will not perform security investigations for only ADP positions. Personnel not requiring access to classified information should not be granted this privilege by controlling authorities.

Page 11, paragraph 2-16b. Add subparagraphs (4) through (5) at the end.

(4) The following guidance applies to DoD military, civilian personnel, consultants, volunteers, and contractor personnel who must access a government computer system in the performance of their official duties.

(a) Critical Sensitive. If an individual performs ADP-I type duties as defined in AR 380-67, paragraph 2-200, the position will be designated as critical sensitive. Personnel in this position include individuals who are directly responsible for the planning, direction, and implementation of the activity’s Information Assurance program. Any individual whose major responsibility is the direction, planning, and design of computer systems (hardware and/or software) also is considered in an ADP-I position. All individuals who can access a computer system during maintenance or operation in such a way as to cause grave damage or realize a significant personal gain are also included in an ADP-I position. As a minimum, specific positions which will be designated as critical sensitive are the MACOM Information Assurance Program Manager, MSC and installation Information Assurance Managers, MSC and installation Directors for Information Management, and supervisory personnel of computer hardware and/or software development activities.

(b) Non-critical Sensitive. If an individual performs ADP-II type duties as defined in AR 380-67, paragraph 2-200, the position will be designated as non-critical sensitive. This includes individuals who are responsible for the direction, planning, design, operation, or maintenance of computer systems (hardware and/or software) and whose work is technically reviewed by a higher authority of the ADP-I category to ensure system integrity. Positions requiring this designation include mainframe/minicomputer operators, systems programmers, hardware designers and developers, installation/activity systems administrators, network security officers, Information Assurance Security Officers, password managers, auditors (of system audit trails), and anyone else with root access privileges. Note: Individuals who use a computer are not considered responsible for their “operation” unless they meet the additional criteria described above.

(c) Non-Sensitive. All individuals, who use a computer as an administrative tool, regardless of classification of data being accessed, are performing ADP-III type duties. However, only those individuals who do not access classified information can be considered for non-sensitive position designation. These individuals are “end users” and do not have root access or perform computer security-related functions for their organization.

(5) Investigative requirements will be determined based on the position sensitivity. In addition to assessing an individual’s

computer access privileges, AR 380-67, paragraph 3-101, reference 1b., must be reviewed to determine if criteria other than the ADP category require a more restrictive position sensitivity designation. As an example, an end user of an unclassified computer system performs ADP-III type duties; however, if this individual is authorized access to TOP SECRET information, the position must be designated critical sensitive.

Page 11, paragraph 2-16e. Add subparagraphs (1) and (2).

(1) No waivers from a completed security investigation will be granted for any person being assigned to an ADP-I position.

(2) Waivers from a completed security investigation for persons being assigned to an ADP-II or ADP-III will be considered only if the following conditions are met and included, in writing, in the request for waiver to the DAA.

(a) All requested investigative documentation has been submitted to the appropriate investigative agency.

(b) A local files check has been completed, and potentially derogatory information is brought to the attention of the DAA, in writing.

(c) The first 0-5 level commander or civilian equivalent in the chain of command of the individual has endorsed the decision, in writing.

(d) The decision is documented and endorsed by the senior security manager, in writing.

Page 11, paragraph 2-17. Add subparagraphs e, f and g after subparagraph d.

e. AMCMI is the approval authority for granting access to all foreign nationals and foreign representatives to AMC information systems; all requests will be sent to HQ AMC, ATTN: AMCMI with a copy furnished to AMCIO-F.

f. No foreign national will be granted a waiver from a security investigation for access to any ADP-I, ADP-II, or ADP-III position.

g. U.S. persons (a foreign national with permanent resident alien status possessing a U.S. Government issued “green card”) will be considered for waivers from a security investigation when seeking access to unclassified information systems, to include SBU.

Page 11, paragraph 2-18. Add subparagraph d after subparagraph c.

d. Software Protection.

(1) Government-developed software will be protected per chapter 4, AR 27-60 (Patents, Inventions, and Copyrights). The AMC Intellectual Property Law counsel should be contacted to determine disclosure protection and patent ability for government-developed software.

(2) Storage media will be kept in their protective jackets and stored in the appropriate container according to the sensitivity of the data stored on them.

(3) Backup copies of sensitive data should always be maintained and stored away from work areas. Backup copies of sensitive-but-unclassified (SBU) data must be protected in the same manner as the original data.

(4) On multi-user systems, each user should maintain his/her own storage media. Those data files maintained on the hard disk should be write-protected to avoid damage or manipulation by other users.

Page 11, paragraph 2-19b. Add the following at the end:

AISs that process only sensitive-but-unclassified (SBU) information will use AMC Form 347 (Date) marked “THIS MACHINE IS AUTHORIZED FOR PROCESSING SBU DATA.”

Page 11, paragraph 2-19c. Add the following at the end:

For other protection levels (e.g., FOUO, Privacy Act, etc.), the appropriate regulation will govern the markings used. Storage media containing sensitive Privacy Act data will be marked “FOR OFFICIAL USE ONLY – Privacy Act Data”. The protective jacket will also be appropriately marked if the label on the storage media cannot be seen when the media is placed in its jacket.

Page 12 paragraph 2-19e. Add subparagraph f. through i. after subparagraph e.

f. AMC activity commanders or their functionaries for AIS security will establish local procedures governing accountability control of sensitive AIS input/output media. As a minimum, control will be per current regulatory requirements for handling FOUO and Privacy Act information, as applicable.

g. Working papers. The following classified media may be treated as working papers.

(1) All media, with exception of TOP SECRET media, that are temporary in nature (retained for 90 days or less) and that stay within the confines and control of the AIS facility. This includes media such as tapes and disk packs that are used and updated at frequent intervals. Even though the tape or disk pack may exist as a physical entity for more than 90 days, the data or information is frequently changed and new “media” created at each update. Top Secret media will contain all markings, declassification/downgrading instructions and source of classification upon creation per AR 380-5, paragraph 7-304.

(2) Media received from customers for processing that are returned to that customer following processing. This includes, but is not limited to, coding forms and punch cards.

(3) Hard copy output from an automated system may be treated as working papers if the provisions of AR 380-5, paragraph 7-304, are followed.

h. Record copies. The following classified media will be treated as record copies or finished documents.

(1) Any classified media, other than that described in g.(2) above, that is being transferred to another AIS facility, unit, installation, or activity, by other than electrical means, e.g., sending classified tape through the mail to another activity. In an example such as this, the magnetic tape will be shipped and a receipt obtained, using DD Form 3964 (Classified Document Receipt) as outlined by AR 380-5. When the tape is introduced into the receiving activity, it may be treated as a working paper if the applicable conditions (as stated above) exist.

(2) Hard copy output and other media retained for more than 90 days by any user or customer. It is the responsibility of the user or customer to control these media.

(3) Those media used exclusively within the AIS facility/DPA that contain relatively permanent and unchanging data such as a magnetic tape containing a classified operating system.

(4) All media described in (1) through (3) above will be assigned downgrading or exemption instructions prescribed in AR 380-5.

i. Automated computer-generated briefings are being used more and more. Two of the advantages associated with this technology are portability and exportability. The use of a few relatively simple security precautions will usually counter the vulnerabilities:

(1) All diskettes must be labeled with the appropriate classification of the briefing. Any diskette created in a sensitive compartmented information facility (SCIF) must be protected at the highest level of information stored on the equipment on which it was created. As an example, if an automated system located in a SCIF contains TOP SECRET information, all diskettes created on that piece of equipment must be labeled and protected at the TOP SECRET level.

(2) To reduce the possibility of inadvertently storing classified information on an unclassified briefing diskette, the diskette should be write-protected prior to distribution.

(3) Diskettes containing classified text will be handled and marked per AR 380-5. Both the label on the diskette and its protective jacket must be appropriately marked.

<u>Page 13, paragraph 2-23b</u>. Add the following at the end:

Computer access telephone numbers, Internet Protocol and Uniform Resource Locator addresses will be designated and protected as FOUO.

<u>Page 14, paragraph 2-26</u>. Add subparagraphs f through j after subparagraph e.

f. Standing operating procedures (SOP) will address protection of equipment and information during off-site processing. All government-related work is the property of the U.S. Government. Licensed software copyrights will be strictly observed. Non-sensitive proprietary and sensitive-but-unclassified (SBU) information may be processed off-site provided it is afforded protection from unauthorized use and disclosure.

(1) Resource asset handling and/or distribution programs will not be processed off-site without the approval of the MACOM or Army Staff (ARSTAF) functional proponent.

(2) Laptops used for processing SBU information will be marked with SF 710 “UNCLASSIFIED” on the keyboard side of the computer.

(3) Laptops designated for SBU processing under the provisions of this policy will not be connected to any computer or part of a computer while that system is processing classified information.

g. The AIS security SOP will describe the additional security requirements for laptop/portable computer, to include the following.

(1) Authorization requirements and responsibilities within the AIS concerning movement/removal of AIS equipment.

(2) Documentation requirements (e.g., use of property passes, hand receipts, etc.) prior to removal of the equipment and software from the activity/installation.

(3) Specific security requirements for safeguarding and storage of equipment during periods of off-site processing.

(4) Protection of software, data, and output.

h. Laptop/portable/personal computers in SCIFs.

(1) Laptops or other portable computers, regardless of the classification of the data processed, will not be allowed in and out of a SCIF and should not be procured/obtained for that environment. When the operational mission requires automation support for an individual on official travel, prior arrangements should be made with the site(s) he/she is visiting for the required automation support. For collateral information processing, arrangements should be made to use laptops outside the SCIF(s). For SCI processing, arrangements should be made to use compatible AIS processing capability available at the visited SCIF(s) so that only software/data is transported. Exceptions to this policy will be granted by the HQ AMC Special Security Officer (SSO) on a case-by-case basis under the following criteria:

(a) Approval must be obtained prior to movement of the computer.

(b) The approval request must include the accreditation date of the AIS and accreditation official for the computer(s) involved. Additionally, a statement verifying prior approval from the visited SSO or his/her designee is required.

(c) The laptop must be Government owned.

(d) Laptops with built-in modems are not authorized to be connected to any circuit within a SCIF. Laptops without built-in modems will not be connected to a modem while in a SCIF.

(e) Laptops may not be operated within two meters of any red processor components or metallic conductors, i.e., pipes, conduits, wires, cables, ducts, etc.

i. Program and/or data disk associated with the laptop must be labeled with the highest classification of the data contained therein, including the unclassified label when applicable. A diskette brought into a SCIF will not be taken out unless the SSO or his/her designee has verified that the label properly reflects the diskette’s classification. Any file encrypted with a non-NSA approved cryptographic system will be considered classified to the highest category of information processed within the SCIF. Unless the encrypted file can be reviewed and certified by the IASO or SSO as unclassified, the diskette will not be permitted to leave the SCIF except by approved courier. Files completely encrypted by an NSA-approved cryptographic system will be considered unclassified when encrypted and the COMSEC key is neither stored nor couriered with the encrypted material. Storage media containing software programs and/or data files and information will, regardless of source of ownership, not be removed from a SCIF without the prior coordination and approval of the user’s supervisor and the system IASO.

(1) When equipment approved under these guidelines is removed from a secure area, it must be kept under lock and key when not in the physical possession of the user. It shall be transported and stored in a manner that affords security sufficient to preclude sabotage, theft, or tampering.

(2) To the maximum extent possible, cleared personnel will do laptop computer maintenance. In those instances where the cost of obtaining cleared maintenance personnel is prohibitive, maintenance may be performed by personnel not cleared provided the laptop is used only for processing sensitive-but-unclassified information. Unauthorized repair or modification of laptops is strictly prohibited.

(3) The responsibilities of the SSO or designee consist of ensuring that procedures are developed to carry out these guidelines. It is not necessary for the SSO or designee to personally conduct all the security checks prescribed. However, the SSO or his/her designee must sign the certification that the laptop has been declassified.

(4) These guidelines do not exempt any equipment from the entry or exit checks required by Director, Central Intelligence Directive (DCID) 1/21, Physical Security Standards for Sensitive Compartmented Information Facilities (U). Any diskettes or computer equipment not approved for exit by the SSO or designee will be confiscated. If found during a random check, a security violation will be reported. The SSO or designee may require additional safeguards where necessary.

j. The entry of privately owned telephones, pagers, answering machines, and other communication devices into government workplaces is discouraged. Local standing operating procedures should explicitly specify the policy for entry and use of privately owned electronic communication devices in government workplaces.

Page 14, paragraph 2-27. Add subparagraphs g through m after f.

g. The following types of incidents are considered emergencies and will receive the highest priority when reported to RCERT and the AMC-IAPM:

(1) Possible life-threatening activity

(2) Attacks on the Internet infrastructure, such as:

(a) Root name servers

(b) Domain name servers

(c) Major archive sites

(d) Network Access Points (NAPs)

(3) Widespread automated attacks against Internet sites

(4) Network Sniffers

(5) Router Attacks

(6) Root compromises

h. An incident, which falls into one of the categories listed above, will be reported telephonically to the RCERT at DSN 879-2482 or commercial (520) 538-2482, and the AMC IAPM at DSN 767-3310 or commercial (703) 617-3310 immediately. In addition, to the telephonic notification to the RCERT and the AMC IAPM, the reporting activity will also submit a written report to the RCERT and cc the AMC IAPM using the ACERT incident report form available at http://www.acert.belvoir.army.mil/frames.html. All email reports submitted to HQAMC will be forwarded to amcio-f@hqamc.army.mil, amcio-iapm@hqamc.army.mil and jwilson-galleher@hqamc.army.mil .

i. Incident reports will include, at a minimum, the incident severity (i.e. Immediate, Priority or Routine). All “immediate” and “priority” incident reports, follow-on actions taken, and the final report will be submitted to the AMC IAPM.

j. The CONUS RCERT can be reached toll free at 1-800-305-3036; by nonsecure fax commercial (520) 538-6809, DSN 879-6809 and unclassified email: rcert@hqasc.army.mil. The Army Network and Systems Operations Center (ANSOC) Help Desk is located on the Web at www.ansoc.army.mil and telephonically at DSN 879-6798, commercial (502) 538-6798.

k. The European RCERT can be reached telephonically at DSN 380-5232, commercial in Germany 0621-730-5232; outside (011-49) 0621-730-5232; nonsecure fax commercial in Germany 0621-730-5252, outside Germany (011-49) 0621-730-5252, DSN 380-5252; secure fax commercial in Germany 0621-730-5061, outside Germany (011-49) 0621-730-5061, DSN 380-5061. The SIPRNET address is 5sig001@66mi.army.smil.mil. Classified email: ur5srs@army.eucom.ic.gov; unclassified email: rcerte@hq.5sigcmd.army.mil. The mailing address is Commander, 5TH Signal Command ATTN: AFSE-IS (RCERT-E) APO AE 09056.

l. The Pacific RCERT can be reached telephonically at DSN (315) 438-7999/1068, commercial (808) 438-7999/1068. Unsecured fax DSN (315) 438-1817, commercial (808) 438-1817. Unsecure email for customer support: pacrcert@schafter-emh3.army.mil. The mailing address is Commander, 516TH Signal Brigade, ATTN: PACRCERT-TNOC, Fort Shafter, Hawaii 96858-5410

m. The Korean RCERT may be reached via email at rcert@usfk.korea.army.mil.

NOTE: Activities requiring access to the ACERT website to report incidents are required to register their domain (.mil and .gov only) at the ACERT. The organization point of contact should send an email to acert@liwa.belvoir.army.mil and have the System Administrator or Domain Name Server (DNS) Administrator invoice the reverse IP Look-up feature on their server. After the preceding procedures are completed, the activity will have the capability to report incidents to the CONUS RCERT through the ACERT website.

Page 15, paragraph 3-1. Add subparagraphs i through k after subparagraph h.

i. The Commander, U.S. Army Aviation and Missile Command, will function as the accreditation authority for all telecommunications AISs (TAIS) operated by Test, Measurement, and Diagnostic Equipment (TMDE) units worldwide.

j. AMC subordinate commands that have activities located in Europe must ensure that those activities forward their accreditation packages to the AMC-Europe Security Office for approval. The AMC-Europe Security Office is responsible for maintaining a complete accreditation inventory of all automated systems located in Europe. This includes those activities that have been given approval to accredit their own systems.

k. The requirements of the DoD 5200.40, DOD Information Technology Security Certification and Accreditation Process (DITSCAP), dated 30 Dec 97, will be met for AIS accreditation. To assist in using the DITSCAP, a Draft DITSCAP Application Document (DoD 5200.40-M) and a DITSCAP System Security Authorization Agreement (SSAA) Automated Tool Prototype are available for downloading at DISA’s Information Assurance Support Environment (http://mattche.iiie.disa.mil).

Page 16, paragraph 3-3b. Add subparagraphs (4) through (5).

(4) Accreditation documentation and risk acceptance statements for small computers may be consolidated by computer type and organization as long as the risk remains the same. Physical limits of any single AIS will be determined by the IAM after considering access controls and processing requirements. Designation of an entire building or floor is discouraged, except in particularly small locations. The intent of the above is to permit multiple AISs, with like risks and vulnerabilities, to be accredited under a single accreditation. For example, functionally similar microcomputers used for SBU email throughout an organization may be accredited together. The computers may be located in different organizational elements, separate buildings, or at multiple locations. As long as all risks and vulnerabilities to the

systems have been identified and acceptable countermeasures are in place, one accreditation statement may be used to accredit the individual AISs. Appendix J provides the minimum accreditation documentation required in accordance with the DITSCAP.

(5) AMC contractors processing SBU information will provide a copy of their security plan (per Public Law 100-235) to their contracting officer.

Page 16, paragraph 3-4f. Add after last sentence:

The certification authority (CA), in accordance with the DITSCAP, will be appointed by the DAA. The CA is normally involved during the material development phase for a system's generic accreditation (DITSCAP phases 1, 2, and 3), not during a system's operational reaccreditation (DITSCAP phase 4). The duties and responsibilities of the CA during each DITSCAP phase are outlined in the DITSCAP Application Document.

Page 16, paragraph 3-5d. Add subparagraphs (1) and (2).

(1) All security plans requiring higher headquarters approval will contain a statement on the forwarding letter that the next lower level accreditation authority has reviewed the package and recommends approval. This applies to those systems which process SIOP-ESI, SCI, and SAP data.

(2) Those systems that process SCI will contain a signed coordination from the local IASO of the SCIF. Accreditation documents will then be forwarded through command channels to HQ AMC, ATTN: AMCMI.

Page 16, paragraph 3-5d. Add subparagraph e after subparagraph d.

e. All AISs that operate under the AMC-approved operational accreditation will be labeled to indicate the classification level at which they are approved to operate.

Page 17, paragraph 3-7. Add the following at the end of the first sentence.

For all accreditation or reaccreditation approved at the MSC/SRA level, the IAM will forward a copy of the signed DAA approval letter to HQ AMC (AMCIO-F).

Page 17, paragraph 3-8a(2). Add the following at the end:
The Commander, AMC, will appoint the Chief Information Officer, HQ AMC, as the designated accreditation authority (DAA) for all Top Secret and below collateral systems operating in the dedicated, systems high, or compartmented security modes. Commanders/directors of MSCs and Separate Reporting Activities (SRAs) are delegated Top Secret and below accreditation and reaccreditation authority within their commands with the authority to delegate as required within the limits of AR 380-19.

Page 18, paragraph 3-8a(4). Add the following at the end:

MSC commanders, SRA commanders/directors (Military rank of 06 and above or civilians GM-15/GS-15 or above) are delegated designated approving authority (DAA) for Top Secret and below collateral system accreditations. The AMCMI is delegated accreditation authority for TS/SCI systems which process in the dedicated mode.

Page 18, paragraph 3-8a. Add subparagraphs (5) through (6) after subparagraph (4).

(5) Installation/activity IAMs will review accreditation packages for accuracy and content prior to forwarding to the accreditation authority. Those installations/activities requiring accreditation approval at HQ AMC will forward their accreditation packages to HQ AMC, ATTN: AMCIO-F. All packages sent to AMC for approval will contain a statement on the forwarding letter confirming the subordinate accreditation authority at the lower level has reviewed the package and recommends approval.

(6) For contractor-owned, contractor-operated (COCO) and Government owned contractor-operated (GOCO) facilities, the approval authority will stay within the Army.

(a) If personnel of the rank of LTC, GM-14/GS-14 or above head the contractor facility, that individual can accredit sensitive-but-unclassified AIS systems (delegation must be in writing).

(b) If the facility has an Army contractor representative only at the site, the appropriate AMC DAA should approve the accreditation.

(c) If the government facility is headed by personnel of the rank of LTC, GM-14/GS-14 or above, that individual can accredit sensitive–but-unclassified systems.

Page 19, paragraph 3-11. Add paragraphs 3-12 and 3-13 after paragraph 3-11.

3-12. Contractors processing Special Access Program (SAP) information
DSS approval to operate a classified AIS facility IAW NISPOM and NISPOM Supplemental Guidance, to include processing of SAP information, satisfies Army/AMC accreditation requirements. This policy should not be construed to mean that additional Information Assurance requirements beyond those required by the NISPOM/NISPOM Supplement and/or DSS cannot be levied on a contractor. The specific additional requirements must be a part of the contract documentation.

3-13. Army facilities processing SAP information
Any system that processes SAP data must be accredited. Accreditation documentation normally will not contain any SAP information. Per AR 380-381 (Special Access Programs (SAPs)), the accreditation documentation will be forwarded through the security office of the command owning and operating the computer to the appropriate accreditation authority. If the accreditation documentation does contain SAP information, the package must be forwarded to the appropriate accreditation authority through SAP channels.

Page 19, paragraph 4-1. Add subparagraph m. after subparagraph l.

m. Use of secure telephones (e.g., STU III, STE, etc.) and accredited microcomputers to transmit classified information –

(1) A STU-III may be used to transmit classified data to another STU-III. Both STU-IIIs must be keyed to the highest level of information to be passed between them (i.e., to pass SECRET data, both STU-IIIs must be keyed to the secure SECRET level). The vulnerability exists that higher level information could inadvertently be passed between the STU-IIIs because there are no checks to determine the classification of data. The operators/users must be aware of this vulnerability and ensure that the data transmitted is classified no higher than what the STU-IIIs are keyed to transmit and receive.

(2) Both computers connected to the secure telephones must be accredited at the highest level of classification of information to be transmitted. If the personal computers (PC) are currently accredited as stand-alone, the systems will require reaccreditation to address communications security.

(3) Prior to transmitting classified information to another PC, accreditation statements must be provided to the various participants.

Page 20, paragraph 4-3c. Add subparagraph d after subparagraph c.

d. Facsimile equipment: Communication protection is waived for the transmission of SBU information, to include "FOR OFFICIAL USE ONLY," on facsimile equipment when:

(1) The sender or receiver is on TDY and is a member of the Armed Forces, a federal employee, or a government contractor, and an authorized facsimile is not conveniently located.

(2) Use of commercial facsimile facilities must be limited to those transmissions considered necessary to the completion of the mission.

(3) The procurement of Data Encryption Standard (DES) equipped or DES-compatible facsimile machines is not required for transmission of SBU information. Specifically, DES is not required for the transmission of time-sensitive information in the form of letters, memoranda, information papers, reports, etc.

Page 20, paragraph 4-4d. Add subparagraphs (4) through (7) after subparagraph (3).

(4) Communication with maintenance personnel to coordinate their activities and provide instruction.

(5) Communications with manufacturing personnel to provide instruction to start, stop, energize, reenergize, and adjust equipment.

(6) Transmission of traffic control information for reporting of accidents, congestion, etc.

(7) For guard forces (non-military), DES-equipped radios are required only at AMC installations or activities where the local threat analysis has identified the need, or when the forces are involved in operations which justify the use of such equipment. When DES-equipped radios are required and are not available for these purposes, guard forces may not purchase commercial encryption equipment without obtaining prior approval from HQ AMC, ATTN: AMCMI.

Page 20, paragraph 4-4d. Add subparagraph e. after subparagraph d.

e. Prior to turn-in of radios (mobile, hand-held, base station, etc.), it is required that all radio frequencies be removed (crystals) or deprogrammed (digital). Personnel responsible for radio maintenance or other appropriate/authorized personnel will document certification.

Page 20, paragraph 4-5a. Add the following at the end:

The authority to approve/accredit protected distribution systems (PDS) is the same as that delegated to accredit automated systems. It is valid for both voice and data systems that process classified information. For data systems that have an associated PDS, the approval process will be handled at the same time as the accreditation of the system.

Page 21, paragraph 5-3d(1). Add the following at the end:

The Foreign Intelligence Officer (FIO) of the organization completing risk assessment (or the FIO at the next higher echelon, if no FIO is available locally) will be contacted to seek current information concerning these threats or threat agents.

Page 21, paragraph 5-3. Add subparagraph i after subparagraph h.

i. The short-form risk assessment included in appendix K may be used for small computer and minicomputer systems. Contracting-out this service or procurement/lease of software is not permitted without written approval from HQ AMC, ATTN: AMCIO-F.

Page 23, Appendix A, Section I Required Publications. Add the following reference:

DOD 5200.40
DOD Information Technology Security Certification and Accreditation Process (DITSCAP)

Page 23, Appendix A, Section II Related Publications. Add the following references:

DODD 5500.7
Standards of Conduct

AMCR 25-1
Electronic Mail

AR 18-22
Army Inventory of Data Systems (AIDS)

AR 27-60
Patents, Inventions, and Copyrights

AR 190-45
Military Police Enforcement Reporting

AR 1-39
Defense Supply Service-Washington

AR 420-90
Fire Protection

AR 710-2
Supply Policy Below the Wholesale Level

DA Pam 25-1-1
Installation Information Services

Page 24, Appendix A, Section III. Add the following:

AMC Label 350
NONSENSITIVE

Page 25, Appendix B, paragraph B-1. Add the following at the end:

Most Federal Government communications systems are not secure. Employees shall not transmit classified information over any communication system unless it is transmitted using approved security procedures and practices (e.g., encryption, secure networks, secure workstations). In addition, employees shall not release access information, such as passwords, to anyone unless specifically authorized to do by the IAM. Employees should exercise extreme care when transmitting any sensitive information or other valued data. Information transmitted over an open network (such as through unsecure email, the Internet, or telephone) may be accessible to anyone else on the network. Information transmitted through the Internet or by email, for example, is accessible to anyone in the chain of delivery. Internet information and email messages may be re-sent to others by anyone in the chain.

Page 25, Appendix B, paragraph B-2. Add the following at the end:

Supervisors are responsible for admonishing employees for using the WWW for other than official business. Supervisors may request DOIM assistance in controlling WWW use for other than official business and authorized personal use. Supervisors’ seeking WWW use guidance should use AMC Policy Memorandum #97-08 with change 1.

Within AMC, a waiver (MEMORANDUM, 13 Feb 96, HQ AMC, AMCMI, subject: Exception to Policy for Encryption of Unclassified-Sensitive 2 Data), has been approved to transmit the following categories of SBU data: logistics, medical care, personnel management, Privacy Act data, contractual data, and "For Official Use Only" information. Information NOT included is SBU information which involves intelligence activities, involves cryptologic activities related to national security, involves command and control of forces, is contained in systems that are an integral part of weapons systems, and is contained in systems that are critical to the direct fulfillment of military or intelligence missions.

Page 25, Appendix B, paragraph B-5. Add the following at the end:

All AMC organizations operating and/or maintaining a bulletin board, ftp server, web server, etc., utilized by any Army organization, including the originating element, will obtain approval to operate the bulletin board, ftp server, web server, etc., from HQ AMC, ATTN: AMCIO-F. Content of the requesting document will include –

(1) Actions taken to prohibit unauthorized users from uploading to the bulletin board, ftp server, web server, etc.

(2) Techniques employed to ensure that software being introduced into a bulletin board, ftp server, web server, etc., have undergone examination for contamination, i.e., code has been examined, software has been tested against a reputable virus detection program, etc.

(3) Methods used to ensure that acquired software for use on the bulletin board, ftp server, web server, etc., do not evoke legal or fee requirements.

Web server software and the software of the underlying operating system shall contain all manufacturer recommended patches. Software patches/fixes will only be applied by the SA in conjunction with the IASO and/or other appropriate personnel.

Page 27, Appendix D, paragraph D-8. Add subparagraph g:

g. When applicable, a completed MOA for use of a privately owned computer will be attached.

Page 30, Appendix G. Add to both subparagrapghs G-1a(2) and page 31, G-2a(2).

A waiver from the use of C2 Protect tools by SAs to periodically review system security may be granted if one of the following conditions apply:

(a) The AIS uses an operating system that has no associated tools.

(b) The cost of porting the tools is prohibitive.

(c) The system already has functionally equivalent tools installed and in use.

(d) The IASO has performed a Risk Assessment and the DAA has made a determination that the use of the tools would not substantially reduce the risk to the system.

(e) Existing centrally fielded systems that are configuration-managed by an organization other than the operating organization will be exempt. In this situation, the operating organization will use the appropriate method to notify the configuration manager of AMC's requirement to have the appropriate tools loaded and used to review system security.

Page 32, Appendix G. Add to end of paragraph G-4a.

All requests for CDAPs will be sent through the AMC chain of command to HQ AMC, ATTN: AMCIO-F.

Page 33. Add Appendixes H through K.

The proponent of this supplement is the U.S. Army Materiel Command. Users are invited to send comments and suggestions for improvement on DA Form 2028, (Recommended Changes to Publications and Blank Forms) to the Commander, USAMC, ATTN: AMCIO, 5001 Eisenhower Avenue, Alexandria, VA 22333-0001.

FOR THE COMMANDER:

OFFICIAL:

CHARLES C. CANNON, JR.
Major General, USA
Chief of Staff

CAROLYN GEBRE
Acting Chief, Printing and
Publications Branch

DISTRIBUTION:
Initial Distr H (45) 1 ea HQ Acty/Staff Ofc
B-Distribution (32)
AMCIO-I-SP (Stockroom) (50)
AMCIO-A (25)

APPENDIX H

MEMORANDUM OF AGREEMENT
BETWEEN

(The Information Assurance Manager and the Individual)

SUBJECT: Information Assurance - Use of Privately Owned Computers

1. Purpose. The purpose of this memorandum is to outline the responsibilities of management and the owner of a privately owned computer when the privately owned computer is to be used for the performance of official duties.

2. References.

a. AR 380-19, Information Systems Security, 27 February 1998.

b. AR 25-1, Army Information Resources Management Program, Chpt 5.

c. AMC Supplement 1 to AR 380-19, Information Systems Security.

3. Intent. The intent of this memorandum is to provide a clear understanding of the responsibilities and liabilities involved in allowing the use of privately owned personal computers for the performance of official duties. Before a privately owned computer can be used, the computer must be approved in accordance with (IAW) AR 25-1, chapter 5, and comply with all provisions of AR 380-19 to include accreditation.

4. Scope. This memorandum will outline the responsibilities of both management and the owner of the privately owned computer. Upon signature by the owner and the Information Assurance Manager, it is implied that use of the privately owned computer for the performance of official duties is necessary and will be of benefit to the organization.

5. Understandings, agreements, support, and resource requirements.

a. The privately owned computer will only be used in a stand-alone configuration, unless specifically approved for communication by the accreditation authority.

b. Only supplies already in the installation supply system may be used. It is understood that the individual will not be reimbursed for the use of his/her own supplies.

c. All information processed on the computer becomes the property of the organization for which it is produced and will be marked accordingly.

d. The privately owned computer will not be used for on-site processing until an accreditation has been completed and approval to operate obtained IAW AR 25-1, chapter 5.

e. Classified defense information will not be processed on the privately owned computer; only sensitive-but-unclassified information may be processed.

f. The owner of the computer waives all rights to claim compensation when performing official duties on the computer.

g. The privately owned computer must be registered with the IAM. This registration will include equipment make, model, serial number, user name, telephone extension, and location, and may be used as an identification pass when moving the computer in and out of the building.

h. The user of the privately owned computer will be designated as an automated information system (AIS) IASO.

i. All privately owned computer equipment brought onto government property will be at the risk of the owner. The government will not be held liable for loss or destruction of any such computer equipment.

j. The owner of the computer is responsible for its physical security.

k. Media on which information is processed on a privately owned computer must be compatible with existing resources. Official file copies must be on a medium which will last for the retention period of the files as specified in AR 25-400-2 (The Modern Army Record Keeping System (MARKS)).

l. Government funds will not be used to purchase hardware accessories or software for privately owned computers.

m. For those privately owned computers already in place in the office environment, paragraphs 5.a. through l. of this memorandum of agreement (MOA) apply.

6. Effective Date. This agreement will be in effect when signed and dated by both the individual and the IAM. It will be reviewed in conjunction with reaccreditation of the AIS to which the individual's equipment has been assigned or upon any changes to the conditions specified within this MOA.

(Signature of Individual) (Signature of IAM)

(Date) (Date)

APPENDIX I

CERTIFICATION, ACCREDITATION AND REACCREDITATION

Systems that had begun operational accreditation under AR 380-19 or were fully accredited prior to the promulgation of the DITSCAP use requirement by HQ AMC on 9 June 1999, remain valid. Each new C&A effort as well as reaccreditation will follow the DITSCAP procedures. For additional DITSCAP information, please refer to the DISA Information Assurance Support Environment at http://mattche.iiie.disa.mil. To access this site, one has to have either a .mil or .gov information systems account.

APPENDIX J

MINIMUM ACCREDITATION DOCUMENTATION REQUIRED

(DOD Information Technology Security Certification and Accreditation Process (DITSCAP), DODI 5200.40, December 30, 1997)

System Security Authorization Agreement (SSAA) Outline

The SSAA is a living document that represents the formal agreement among the DAA, the CA, the user representative, and the program manager. The SSAA is developed in phase 1 and updated in each phase as the system development progresses and new information becomes available. At minimum, the SSAA should contain the information in the following sample format:

1. MISSION DESCRIPTION AND SYSTEM IDENTIFICATION
   - 1.1. System name and identification.
   - 1.2. System description.
   - 1.3. Functional description.
     - 1.3.1. System capabilities.
     - 1.3.2. System criticality.
     - 1.3.3. Classification and sensitivity of data processed.
     - 1.3.4. System user description and clearance levels.
     - 1.3.5. Life cycle of the system.
     - 1.3.6. TCSEC/Common Criteria
   - 1.4. System CONOPS Summary.

2. ENVIRONMENT DESCRIPTION
   - 2.1. Operating Environment.
   - 2.2. Software development and maintenance environment.
   - 2.3. Threat description.

3. SYSTEM ARCHITECTURAL DESCRIPTION
   - 3.1. Hardware.
   - 3.2. Software.
   - 3.3. Firmware.
   - 3.4. System interfaces and external connections.
   - 3.5. Data flow (including data flow diagrams).
   - 3.6. TAFIM DGSA, security view.
   - 3.7. Accreditation boundary.

4. ITSEC SYSTEM CLASS
   - 4.1. Interfacing mode.
   - 4.2. Processing mode.
   - 4.3. Attribution mode.
   - 4.4. Mission-reliance factor.
   - 4.5. Accessibility factor.
   - 4.6. Accuracy factor.
   - 4.7. Information categories.
   - 4.8. System class level.
   - 4.9. Certification analysis level.

5. SYSTEM SECURITY REQUIREMENTS

5.1. National and DOD security requirements.
5.2. Governing security requisites.
5.3. Data security requirements.
5.4. Security CONOPS.
5.5. Security policy
5.6. Network connection rules.
5.6.1. To connect to this system.
5.6.2. To connect to the other systems defined in the CONOPS.
5.7. Configuration and change management requirements.
5.8. Reaccreditation requirements.

6. ORGANIZATIONS AND RESOURCES

6.1 Identification of organizations.
6.1.1. DAA.
6.1.2. Certification Authority.
6.1.3. Identification of the user representative.
6.1.4. Identification of the organization responsible for the system.
6.1.5. Identification of the program manager or system manager.
6.2. Resources.
6.2.1. Staffing requirements.
6.2.2. Funding requirements.
6.3. Training for certification team.
6.4. Roles and responsibilities.
6.5. Other supporting organizations or working groups.

7. DITSCAP PLAN

7.1. Tailoring factors.
7.1.1. Programmatic considerations.
7.1.2. Security environment.
7.1.3. IT system characteristics.
7.1.4. Re-use of previously approved solutions.
7.1.5. Tailoring summary.
7.2. Tasks and milestones.
7.3. Schedule summary.
7.4. Level of effort.
7.5. Roles and responsibilities.

8. APPENDICES

8.1. Appendix A Concept of Operations Diagram
8.2. Appendix B Threat Statement
8.3. Appendix C Hardware/Software Environment
8.4. Appendix D ITSEC System Class
8.5. Appendix E Certification Analysis Level
8.6. Appendix F Verification Phase Certification Tasks
8.7. Appendix G Validation Phase Certification Tasks
8.8. Appendix H Technical and Non-Technical Security
8.9. Appendix I Certification Team member Roles and Responsibilities
8.10. Appendix J Tasks and Milestones
8.11. Appendix K Schedule Summary
8.12. Appendix L SSAA Roles and Responsibilities
8.13. Appendix M Appointment Orders
8.14. Appendix N Standing Operating Procedures
8.15. Appendix O Technical Security Configurations of Devices Enforcing a Security Policy

8.16. Appendix P Configuration Management Plan
8.17. Appendix Q Results from Verification Phase Certification Analysis
8.18. Appendix R Risk Management Review
8.19. Appendix S Certification Test/Plan Procedures
8.20. Appendix T Certification Results/Recommendations
8.21. Appendix U Waivers
8.22. Appendix V Accreditation Statement

Optional appendixes may be added to meet specific needs. Include all documentation that will be relevant to the systems' C&A.

Acronym list
Definitions
References
Security Requirements and/or Requirements Traceable Matrix
System Rules of Behavior
Contingency Plan(s)
Security Awareness and Training Plan
Incident Response Plan
Memorandums of Agreement - System Interconnect Agreements
Applicable System Development Artifacts or System Documentation

APPENDIX K
MINIMUM CRITERIA FOR CONNECTION TO AMC NETWORK INFRASTRUCTURE

1. This appendix outlines the process to be taken by the CIO prior to granting connection to the network infrastructure. Figure 1 illustrates the methodology for granting connection to the AMC network infrastructure.

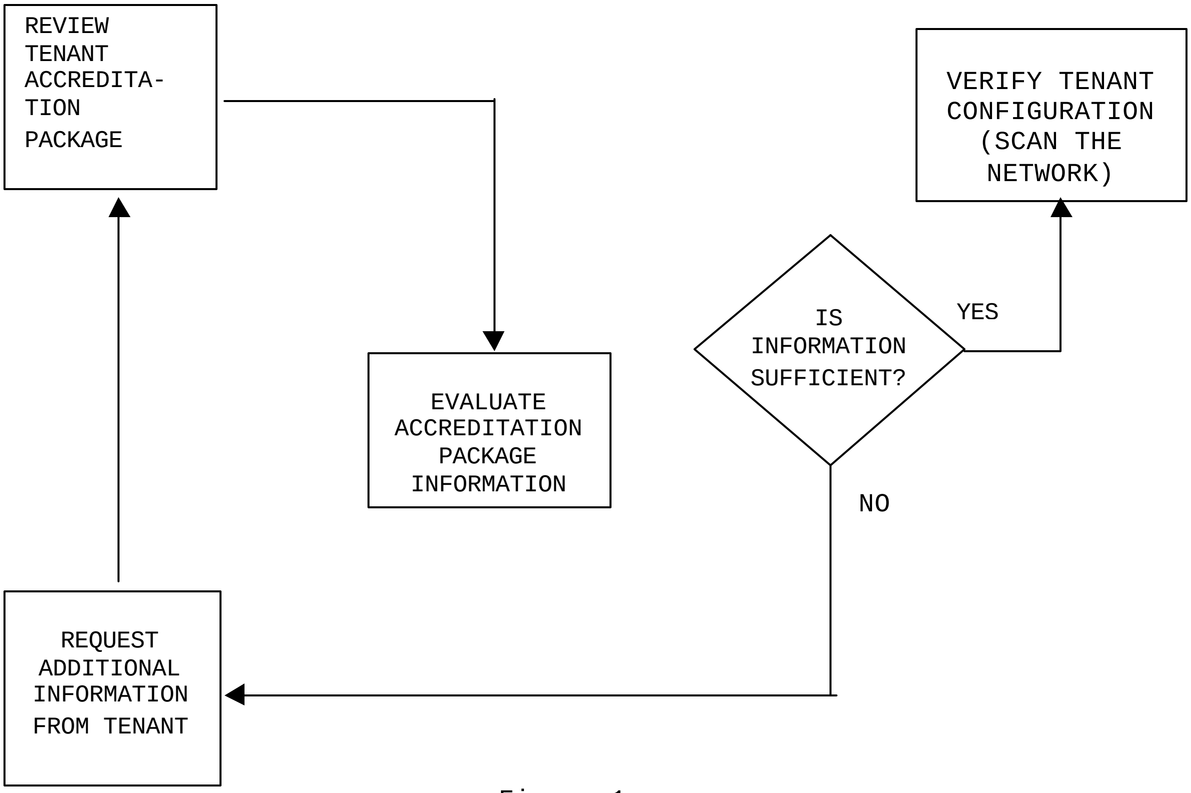
REVIEW TENANT ACCREDITATION PACKAGE
EVALUATE ACCREDITATION PACKAGE INFORMATION
IS INFORMATION SUFFICIENT?
YES
VERIFY TENANT CONFIGURATION (SCAN THE NETWORK)
NO
REQUEST ADDITIONAL INFORMATION FROM TENANT

Figure 1.

Methodology for Granting Connection to the AMC Network Infrastructure

1.1 The Army Materiel Command Authority. The AMC installation CIO will maintain full control and exercise authority over the installation backbone/LAN connections. The installation IAM is a member of the installation CIO staff.

1.2 Tenant Criteria. Any AMC or non-AMC tenant command must adhere to the following:

a. The tenant will provide a description (i.e., pictorial and narrative) to the CIO of the tenant network being connected. This description will show the IP addresses assigned to each hub, bridge, router, and switch connected to the network and all external connections (e.g., dial-up to internet providers or access for remote users) and their locations. Additionally, the description should strive to associate IP subnetworks to physical segments for hub, switches, etc. Any system updates or changes to the tenant network will be provided to the CIO for approval/incorporation into the installation map.

b. The tenant activity will provide a copy of the accreditation package signed by the activity's equivalent DAA to be kept on file by AMC. This package should consist of the following documents:

(1) Certification Statement.
(2) Certification Report of Findings (CROF)
(3) Certification Evaluation Report (CER)
(4) Security Risk Management Review (SRMR)
(5) System Security Requirements Specification (SSRS)
(6) Certification Appointment Letter
(7) Certification Plan

c. Each document is supported by analysis and evidence contained in the preceding document.

(1) The CROF is the "top level" certification document, where the recommendation to either use the system or not is made. The CROF links the results of the CER to the vulnerabilities discussed in the SRMR; the intended audience is the DAA. In contrast, the CER is more technical in nature and contains the actual data and forms the foundation for certification.

(2) The SRMR addresses the risks, vulnerabilities, and possible countermeasures of the entire system. The SRMR is the "living" document that changes as the residual risk in the system is reduced as the System and Security engineers implement countermeasures.

(3) The SSRS is produced by the System and Security Engineer for the system under development. The SSRS is the basis for certification because it tells which security requirements are levied against the system, and is included in the Certification Package for reference.

(4) The Certification Appointment Letter is written by the DAA appointing the Certification Authority who oversees the day to day activity of the evaluation.

(5) The Certification Plan sets forth the goals and procedures for achieving certification/accreditation for the system.

d. By building on the previous document, this ensures a "bottom-up" approach to accreditation.

e. The tenant activity will immediately notify the CIO of significant or security-related changes to the network or external connectivity.

1.3 Compliance with the Criteria. After negotiations, the AMC installation CIO and the tenant organization will sign a memorandum of agreement (MOA) for the specific conditions allowing the tenant to connect to the network infrastructure. By signing the MOA, the organization's connection to the infrastructure network constitutes consent to announced and unannounced verification of security features. Methods of verifying security features include automated vulnerability scanning, modem identification scanning, and physical inspection. These scans are not to be an attack on the network, but will be a normal probe to check for compliance with the connection evidence provided and described in paragraph 1.2. The procedure to obtain connectivity to the AMC network infrastructure includes the following procedures.

a. Tenant submits an Accreditation Package
b. CIO evaluates the package for completeness
c. CIO and Tenant enter into MOA negotiations
d. MOA is signed
e. MOA terms are verified
f. Architecture adjustments are made
g. CIO verifies compliance

1.4 Result of Non-compliance. Failure to comply with this security policy, ARs, and/or DOD memorandums may result in disconnection from the network infrastructure. Refer to AR 380-19, paragraph 1.6f for host installation and tenant requirements. The AMC CIO makes the final decision.

1.5 General Network Security Standards for Interconnection Devices. The following paragraphs outline minimum-security practices concerning interconnection devices (routers, bridges, switches, and modems). These devices connect LANs to LANs, LANs to WANs and LANs to remote devices. The AMC CIO will ensure, as a minimum, the following security practices are employed by the tenant activity.

a. Passwords. Passwords are the first step in controlling access to devices on a network. Passwords force users to identify and authenticate themselves. The following password criteria must be met:

(1) All devices will be password protected.

(2) All default passwords will be changed.

(3) All known unsecure user names and passwords will be removed.

(4) Accepted password creation (e.g., password generators, user-defined 8-character password with upper/lower case, alphanumeric, special characters, etc) will be employed to create passwords.

(5) The IASO or IANO will record the passwords used on communication devices and store them in a secure or controlled manner.

(6) The IASO or IANO will change the password immediately and restrict by IP address if in-band or remote management is required.

b. Device Management. Before adding a device to the network, the following criteria must be met:

(1) Devices will be managed through direct connection or approved secured connection procedures.

(2) The use of remote management will be limited to emergency situations or on a case-by-case basis.

(3) Image files loaded via the trivial file transfer protocol (TFTP) process will be protected from corruption and checked on a monthly basis. The use of Transmission Control Protocol (TCP) Wrappers will restrict access.

(4) Communication will be restricted between devices and the TFTP server to known authorized IP addresses.

(5) Digital signatures or encryption, if available, will be used on the devices supporting Simple Network Management Protocol (SNMP).

(6) All ports except those needed to support the mission will be disabled.

(7) All changes regarding settings and enhancements will be audited and recorded.

c. External Circuits. External circuits are connections to the network by either AMC or non-AMC tenant commands. The following criteria must be met:

(1) All external connections will be validated and approved prior to connection. Efforts will be made to prevent unauthorized external connection to the network.

(2) The IANO shall keep all infrastructure diagrams updated to show all external connections before actually connecting them. These diagrams should be based on a physical or automated inspection of the network.

(3) All undocumented network connections discovered during any inspection will be investigated. Unjustified connections will be disconnected.

(4) Remote access will be secured by Terminal Server Access Control System (TSACS) or an equivalent.

d. Access Control. Access control is necessary to prevent unauthorized access by identifying and authenticating users. After a user is identified and authenticated, access control will allocate the assigned privileges/accesses assigned by the SA. The following criteria must be met:

(1) Access control lists will be established to restrict traffic to and from only authorized addresses.

(2) Disable the IP alias command option.

(3) Ensure only required protocols are accepted at the router.

(4) Locate interconnection devices within controlled access

areas.

(5) Establish and maintain IP filtering

e. Audit. An audit records user access into a system and all actions taken by the user. Audit logs will enable an SA to accurately trace a user’s path through the network or system, including files accessed, modified, and/or deleted. Audits also record any attempted access made by unauthorized users.

(1) Implement appropriate audit related functions in conjunction with an audit repository system.

(2) Review audit logs on a periodic basis, not to exceed one week.

1.6 Use of the AMC Network. To preclude poor operational or security practices by the tenant organization impacting the AMC infrastructure, the tenant activity will ensure the following information is incorporated within their standing operating procedure (SOP) and/or Security Policy (SP). This information should be used to augment, not replace, existing documents.

1.6.1 Acceptable Use of the Network Resources. It is acceptable for authorized user of the network to:

a. Load and execute software applications purchased with government funds, or developed and tested specifically for the government, or legally licensed to the government for official use.

b. Use the network to access and use Internet resources for professional development purposes, subject to ensuring that primary duties and mission are accomplished.

1.6.2 Unacceptable Use of the Network Resources. It is unacceptable for anyone to:

a. Attach network components to the network (e.g., network interface cards (NIC), network printers, single modems, and networkable facsimiles, etc.) without notifying the SA/IANO.

b. Access accounts or resources not required in the performance of normal duties specifically granted by the owner or local IASO.

c. Attempt to ‘crack’ passwords to gain access to any network resource.

d. Attempt to browse information for which a need-to-know does not exist.

e. Disrupt service to other network resources.

f. Share passwords with other users.

g. Violate the copyright or license agreement of any software.

1.6.3 Restricted Use of the Network Resources. The following user restrictions apply for access to network resources:

a. User access is restricted on a “need-to-know” basis. The use of passwords and permissions will enforce this policy.

b. Inbound connection requests (requests from computers outside of the AMC network) will be restricted. This includes connection via a remote connection (modems or other Internet Service provides from home or while on travel status). The IANO reserves the right to refuse connection to any violators.

c. Anonymous access to global information services will be granted ‘read only’ privileges except as designated by the NSO.

d. All software and files down-loaded from non-government sources via the Internet (or any other public network) must be screened with virus detection software. This screening must take place prior to the files being run or examined via another program such as word-processing packages.

1.7 Authorization to Grant and Terminate Access to Services. The IASOs are authorized to grant and terminate access to AMC network services physically contained within their directorate. The IASOs will notify the AMC network center when access is to be terminated or granted.

Page 34, Glossary, Section I. Add the following acronyms:

CA
Certification Authority

CIC
Corporate Information Center

CIO
Chief Information Officer

COCO
Contractor-owned, Contractor-operated

COOP
Continuity of Operations Plan

DITSCAP
DOD Information Technology Security Certification and Accreditation Process (DoDI 5200.40)

DSS
Defense Security Service

FOIA
Freedom of Information Act

FSP
Facility Security Profile

GOCO
Government owned, Contractor-operated

IDS
Intrusion Detection System

MDEP
Management Decision Package

MEVA
Mission Essential/Vulnerable Area

OCC
Operations Center Columbus

RDT&E
Research, Development, Test, and Evaluation

SBU
Sensitive-but-Unclassified

SRA
Separate Reporting Activity

SSAA
System Security Authorization Agreement

TAIS
Telecommunications AIS

TMDE
Test, Measurement, and Diagnostic Equipment

Page 35, Glossary, Section II. Add the following terms:

Automated Data Processing (ADP) facility
An ADP service center designed, built, or installed specifically to provide centralized ADP services. Normally, the ADP facility is identified with a TDA, TO&E fixed site, or mobile site that provides required services for data automation support. Typical ADP facility staff management functions are planning, budgeting, security, training, AIS operations, systems analysis, and programming.

Certification Authority (CA)
The official responsible for performing the comprehensive evaluation of the technical and non-technical security features of an IT system and other safeguards, made in support of the accreditation process, to establish the extent that a particular design and implementation meet a set of specified security requirements.

Corporate Information Center (CIC)
An AIS operation office/organization primarily responsible for the Information Mission Area (IMA) program which encompasses automated information systems, communication, visual information, libraries, and records management for an installation or specific geographic area.

Corporate Information Officer (CIO)
The directing authority of the CIC

Data Processing Activity (DPA)
An AIS operation distributed to a functional user that does not provide the support services of an ADP facility or supports users outside the principal office. Within AMC, the IAM may define a DPA as any room or facility containing AIS equipment and/or storage media or may define a DPA based upon organizational structure and/or mission element. A minimum but adequate number of DPAs must be established. A standard number would be one DPA for each directorate, laboratory, or office. Establishing additional AISs will be at the discretion of the IAM.

Exceptions
An exception will provide long-term relief from a regulatory requirement. Requests for exceptions must be approved only when corrective action of a deficiency is not feasible or when the security afforded is considered equivalent to or better than that provided by regulatory requirements. The accreditation authority will be required to revalidate exceptions every three years from the date of approval or last revalidation. All requests for exception to policy will be routed through the appropriate chain of command to HQ AMC, ATTN: AMCMI.

Facility Security Profile
Hardware/software inventory list

Foreign national
A foreign national is any individual who is not a U.S. citizen by birth or naturalization.

Foreign representative
A "foreign representative" is a U.S. citizen or alien who works for a foreign-owned company. If the individual who works for a foreign-owned company is a U.S. citizen, higher headquarters approval is not required to permit the person access to automated information systems. If the individual is a foreign national, approval is required prior to permitting the individual any access.

Government owned, Contractor-operated (GOCO)
A Government owned facility that is operated by a contractor.

Immigrant alien
An immigrant alien is any person not a citizen of the United States who is under an immigration visa for permanent residence.

Independent terminal facility
Any computer facility containing a portable or stand-alone terminal or word processor, intelligent or dumb, that is not hard wired to a host computer.

Minicomputer
A multiuser computer designed to meet the needs of a small organization or a department/division in a large organization.

Privately owned software
Commercial software purchased by an individual.

Public domain software
Software that has been made available for use without the requirement of licensing and no registration fee is requested.

Sensitivity determination
The method used to determine the sensitivity of data to be processed on the AIS. Sensitivity determination will be accomplished prior to risk assessment and accreditation. It will be used to determine if formal accreditation is necessary. If the AIS meets the criteria for accreditation, or a risk acceptance, a risk assessment will then be performed and become a part of the formal accreditation package.

Shareware
Software for which a registration/use fee is requested, but not required.

Small computer (microcomputer)
Any single-user computer with an arithmetic-logic unit and control unit contained on one integrated circuit (a microprocessor); often called a personal computer or PC.

Superseded software
Software that has been replaced with an update or software that has expired.

Waivers

A waiver provides only temporary relief from compliance with prescribed standards. Requests for waivers are appropriate if corrective actions can be reasonably accomplished within a specific period of time. Waivers apply only to those regulatory requirements which the requester intends/expects to correct within the accreditation period. Waivers cannot be extended past 180 days unless HQ AMC, ATTN: AMCIO-F, grants an exception to policy. Specific waivers may be included in the accreditation package when certain requirements cannot be met because of economical, technical, or operational reasons. As an example, some operating systems do not provide random password generation. A waiver, as part of the accreditation package, would be requested to allow the use of an alternative method to generate passwords. This type of waiver, which may be approved by the accreditation authority, is valid for the length of the accreditation. Waivers requiring approval by higher headquarters or other agencies will be included as an attachment to the security plan. The security plan may not be approved until the waiver has been granted.